

## EFFICIENT PACKET ENCRYPTION METHOD

### Abstract

The present efficient packet encryption method decreases the computation time to encrypt and decrypt successive packets of plaintext data. An S-vector is generated and the S-vector is used to encrypt successive packets of plaintext, thus reducing the per packet encryption/decryption time. The formula for encrypting successive packets includes use of the packet sequence number with a third variable injected to eliminate the predictability of the variables, thus making the present efficient packet encryption method more secure. A fourth variable is injected into the calculations to generate an encryption stream that does not repeat as frequently to provide additional security from hackers. For encrypting a packet having a long payload of plaintext, a packet byte sequence number is used to generate an encryption stream that is less likely to repeat within a particular packet.